EXHIBIT F

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware Corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia Corporation, and SYMANTEC CORPORATION, a Delaware Corporation, Defendants and Counterclaim-Plaintiffs.	)	C. A. No.: 04-1199 (SLR)

EXPERT REPORT OF DANIEL TEAL

TABLE OF CONTENTS

I. INTRODUCTION

1. I, Daniel M. Teal, am the Co-Founder and President of CoreTrace Corporation, a computer security corporation that specializes in providing scalable, secure, Enterprise Computing Management (ECM) systems.

2. I have been retained by counsel for Symantec Corporation as an expert witness in this action. If called to testify as to the truth of the matters stated herein, I could and would do so competently.

II. QUALIFICATIONS

3. I received a Bachelor of Science degree in Electrical Engineering from the Massachusetts Institute of Technology in 1989. I undertook additional computer-related graduate work at the University of Texas at San Antonio from 1992 – 1994.

4. I was the Co-Founder and Chief Scientist of the WheelGroup Corporation (WheelGroup). Beginning in December 1995 – March 1998, WheelGroup designed and implemented the NetRanger Security Management System, one of the first network-based intrusion detection systems. WheelGroup was acquired by Cisco Systems, Inc. in March 1998 for $124 million in stock. From March 1998 – August 1999 I served as a senior software engineer for Cisco Systems, Inc., where I was responsible for research and development tasks to enhance the network security product line including the NetRanger product.

5. At the WheelGroup, I was both the main system architect and the primary software engineer/developer for the initial versions of the NetRanger product. In particular, I wrote the NSX and communications components of the software. I also wrote the majority of the Director software with the exception of the interface with HP Openview network management software. By version 2.0 of NetRanger, the WheelGroup had added additional software developers, but I still served as the primary architect and developer.

I understand that claim language is generally construed in accordance with its ordinary and customary meaning to those skilled in the relevant art as of the date of the invention.[1] I also understand that claim terms should be given the meaning that is objectively discerned from the specification and/or the prosecution history by one of ordinary skill in the art as of the date of the invention, even if that meaning differs from the term's ordinary and customary meaning.

11. I have reviewed an extensive body of prior art publications as well as certain embodiments of the NetRanger software. A list of the prior art publications, documentation, and software embodiments I have reviewed and the individuals with whom I have spoken in forming the opinions set forth below is attached as Exhibit B. Exhibit B also lists the Bates ranges for each document discussed in this report, which I understand designates the version of the document produced in this litigation.

IV. NETRANGER DOCUMENTATION PUBLICLY AVAILABLE PRIOR TO NOV. 9, 1997

12. The NetRanger Security Management System, ("NetRanger") was and is a real-time network security management system for detecting, analyzing, responding to, and deterring unauthorized network activity. Versions of NetRanger have been available commercially since 1996.

13. As a co-founder and past Chief Scientist of the WheelGroup which created NetRanger, I have first-hand knowledge of the functionality of successive NetRanger

[1] "As a starting point, we give claim terms their ordinary and accustomed meaning as understood by one of ordinary skill in the art. ... Accordingly, a technical term used in a patent is interpreted as having the meaning a person of ordinary skill in the field of the invention would understand it to mean." *Bell Atlantics Network Servs., Inc. v. Covad Comm. Group, Inc.*, 262 F.3d 1258, 1267-268 (Fed. Cir. 2001). *See also Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005) (en banc).

product embodiments as well as the documentation, presentations, and press releases prepared by WheelGroup and others about NetRanger. In addition, I maintained detailed files of product descriptions and documentation from December 1995, when I first began working on NetRanger, through March 1998, when the product was sold to Cisco Systems. In order to ensure that my recollection of the details of each of the NetRanger versions discussed below was correct, and that my recollection of the dates of the release of each of the documents listed below was correct, I searched my own personal files to find copies of various press releases, presentations, User Guides and Manuals, and other documentation developed by WheelGroup and others. In addition, I spoke to former WheelGroup colleagues Scott Olson, Scott Waddell, Kevin Wiley, and Jerry Lathem to further verify that my recollection of past events was correct. I also reviewed archived versions of the WheelGroup website (www.wheelgroup.com) from the Internet Archive to further confirm my recollection of when certain documents were posted to the WheelGroup website.

A. NetRanger User Guides and other software manuals

1. NetRanger User's Guide Version 1.3.1

14. The NetRanger User's Guide Version 1.3.1 [SYM_P_0074948-SYM_P_0075282] was publicly available prior to August 25, 1997. The document itself is marked "Copyright © 1997 WheelGroup Corporation." Furthermore, version 1.3.1 of NetRanger was released prior to version 2.0, and an official WheelGroup press release from my files indicates that WheelGroup released version 2.0 on August 25, 1997. [SYM_P_0074722-SYM_P_0074723].

15. This User's Guide was provided along with each sale of the NetRanger product version 1.3.1. In addition, if asked by a potential customer the WheelGroup provided copies of their user manuals upon request. NetRanger version 1.3.1 was sold commercially by WheelGroup. WheelGroup customers who purchased the system

include the US Air Force, IBM, AT&T, Storage Tek, NetSolve, Network General, and BTG. Attached at Exhibit C is a WheelGroup customer list identifying the companies that purchased different versions of NetRanger.

2. NetRanger User's Guides (earlier versions)

16. Each of the following versions of the NetRanger User's Guide were also available publicly prior to August 25, 1997, and were provided along with each sale of the NetRanger product of the same version:

- NetRanger User's Guide, WheelGroup Corporation, 1996. [SYM_P_0526566-SYM_P_0526735]
- NetRanger High-Level Overview, Version 1.1, WheelGroup Corporation, 11/1996 [SYM_P_0531123- SYM_P_0531139].
- NetRanger User's Guide Version 1.2.2, WheelGroup Corporation, 1997 [SYM_P_0075283- SYM_P_0075535].
- NetRanger User's Guide Version 1.2, WheelGroup Corporation, 1997 [SYM_P_0071736- SYM_P_0071953].

3. Data Privacy Facility / BorderGuard

17. The NetRanger product was designed to work with the NSG BorderGuard security device, which provided virtual private network (VPN) capabilities for NetRanger communications. The Data Privacy Facility Administrator's Guide, DPF Version 1.2, Network Systems Corporation, 9/1995 [SYM_P_0072419- SYM_P_0072641] explains the cryptographic component of the BorderGuard security device. This document was publicly available as of September 1995, when it was provided along with each NSG BorderGuard security device sold commercially. In addition, as indicated at page iii of the DPF Version 1.2 Guide, both a Reference Manual and an Installation Guide were also available for the BorderGuard router itself as of September 1995. Exhibit B contains a list of additional BorderGuard manuals that were publicly available prior to November

1997. Documentation from the Internet Archive from www.network.com [SYM_P_0600799-0600839] further confirms my recollection that multiple versions of the BorderGuard router were publicly available prior to November 1997.

4. HP OpenView

18. The NetRanger product was also designed to operate in conjunction with HP OpenView. HP OpenView was a very well-known network management software application. Up until late 1997, all NetRanger customers were required to purchase a copy of HP OpenView. (NetRanger eventually supported customers using the IBM Netview application as well, and later developed a NetRanger user interface instead of requiring customers to purchase HP OpenView). Thus, I am generally familiar with the sales and marketing of HP OpenView in the 1996-1998 timeframe. Although NetRanger ran on the Unix version of HP Openview, I believe that the major functionality of HP OpenView was similar between the Unix and Windows versions. I know that the HP OpenView product was sold with user manuals, and I would expect that the HP OpenView for Windows User Guide Version 6.1 for Windows [SYM_P_0080944-SYM_P_0081098] would have been publicly available with HP OpenView products as of the October 1997 date indicated in this manual.

B. NetRanger Slides

19. In addition to selling the NetRanger product itself and associated documentation, the WheelGroup also provided training seminars to train customers and potential customers on how to set up and use NetRanger. In April 1997, the "NetRanger Installation & Configuration Training" slide presentation consisted of the documents at [SYM_P_0077338- SYM_P_0077416]. These slides were publicly shown to customers beginning in April 1997. These training sessions were open to any customer who signed up for one of the multiple sessions offered per year. Customers receiving training include the US Navy (May 1997), AT&T (May 1997), American Express (Sept. 1997), and IBM

(Aug. 1997). Each of these customers was shown the "NetRanger Installation & Configuration Training" slide presentation.

C. SQL Queries

20. The SQL queries given at [SYM_P_0074926- SYM_P_0074947] were publicly available as of May 28, 1997. The functionality of these SQL queries was also described, for example, in the NetRanger User's Guide Version 1.3.1 at p. 5-36 [SYM_P_0075174]. These SQL queries were included in source form with the NetRanger product starting with version 1.2. All NetRanger customers of version 1.2 and later could have viewed these SQL queries as part of the NetRanger product that they purchased.

D. DoD Spock Report

21. In March 1997, a Department of Defense-sponsored consortium of both government and commercial organizations performed a detailed evaluation of the capabilities of the NetRanger product. This group, including the National Security Agency, was known as the Security Proof of Concept Keystone (SPOCK). The results of the SPOCK evaluation were documented in a detailed report entitled "NetRanger Real-Time Network Intrusion Detection Performance and Security Test," DoD/SPOCK, including Appendices A, B and C, 4/30/1997 [SYM_P_0074255- SYM_P_0074481].

22. On July 8, 1997 the WheelGroup issued a press release entitled "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger intrusion detection system." [SYM_P_0074647-SYM_P_0074648; SYM_P_0074525-SYM_P_0074526]. As part of this press release, the WheelGroup notified the public that the underlying report documenting the SPOCK evaluation could be obtained by writing to COACT, Inc. 9140 Guilford Road, Suite L, Columbia, MD 21046. Thus despite the SPOCK report being marked "For Official Use Only" the document was made available to members of the public upon request and is therefore not confidential. See also Minutes of SPOCK

meeting, 12/12/96, noting "the resulting test will be made available to all requesters." [SYM_P_0074461].

E. AFIWC Assessment

23. From October to December of 1996, the Air Force Information Warfare Center (AFIWC) performed an extensive test of two different NetRanger configurations. The resulting report was entitled "Product Security Assessment of the NetRanger Intrusion Detection Management System Version 1.1," AF Information Warfare Center, February, 1997 [SYM_P_0074527- SYM_P_0074566].

24. It is my understanding that this report was not classified and was available via Freedom of Information Act (FOIA) requests. The WheelGroup had multiple internal copies of this document and it was not treated as confidential. This report was certainly available to government customers of NetRanger as well.

F. WheelGroup Press Releases

25. The WheelGroup made periodic press releases to inform the public about its products, including NetRanger. These press releases were published on the company's website at www.wheelgroup.com. A summary of when each press release was posted is given in "WheelGroup Press Release Summary" [SYM_P_0074525 SYM_P_0074526].

26. In particular, the press release entitled "WheelGroup Releases NetRanger Version 2.0" was published on the WheelGroup website on August 25, 1997. [SYM_P_0074722-SYM_P_0074723]. In addition, the press release entitled "Summary of DoD/SPOCK Evaluation of WheelGroup's NetRanger intrusion detection system" was published on the WheelGroup website on July 8, 1997. [SYM_P_0074647-SYM_P_0074648].

V. FUNCTIONALITY OF THE NETRANGER PRODUCT AS OF NOV. 9, 1997

27. The NetRanger product as of November 1997 was a well-developed commercial product that had already undergone several different version upgrades to enhance its feature set and functionality. NetRanger was a network security management system capable of operating in real time, which meant that potential intrusions and suspicious activity were detected on the fly, as traffic flowed through the network being monitored. NetRanger operated in TCP/IP networks and could function in a distributed fashion across large networks or multiple sites interacting across the Internet.

28. NetRanger was designed to work with other commercially-available products, such as the BorderGuard security device, and both the HP OpenView and IBM NetView network management systems.

29. The BorderGuard product from Network Systems Corporation circa 1997 was a router / packet filter that was capable of filtering a full set of protocols, including but not limited to the IP protocol. BorderGuard also included sophisticated encryption and VPN capabilities, allowing traffic to be passed securely even over the Internet.

30. NetRanger also integrated with and required the functionality of certain network management systems. Network management systems were used to manage and properly display the data collected from NetRanger sensors. NetRanger required a user to purchase either HP OpenView or IBM NetView in order to use the Director functions of NetRanger.

31. The basic NetRanger system was composed of three main "core" systems that interacted to detect, analyze, respond to and deter unauthorized network activity: the NSX, the Communication System, and the Director.

32. The Network Security eXchange (NSX) system included a Packet Filtering Device subsystem and a Sensor subsystem, and provided the capability to capture network traffic and analyze it to detect suspicious activity. The Packet Filtering

Device component plugged into a network as a router or a bridge, and routed network traffic to the Sensor. The Sensor component contained NetRanger's real-time intrusion detection and content assessment logic. The Sensor's intrusion detection engine contained a large set of different rules, or signatures, capable of detecting a wide assortment of attacks such as sendmail attacks, ping sweeps, IP source routing and spoofing, FTP and Telnet abuse, and SATAN attacks. Sensor analyses produced event records of detected attacks and alarms which were automatically sent on to a Director.[2] The Sensor also accepted intrusion response and reconfiguration information from a Director. An individual NSX could communicate with more than one Director if desired.

33. The NetRanger Communication System included the so-called "post office" subsystem and an Encrypted Sleeve. The post office provided a communication backbone for remote monitoring and transmission of information between the NSX and the Director. The Encrypted Sleeve provided secure data transmission between remote networks and the various NetRanger components by creating a virtual private network (VPN) between each component using the Data Privacy Facility (DPF) that came with Network Systems Corporation's BorderGuard devices. As noted previously, NetRanger was designed to operate in conjunction with the BorderGuard security device. The BorderGuard security device could be installed in various different places on the network being monitored.

34. The Director provided integration and analysis services to NetRanger, and communicated with one or more NSXs via the communication system. The Director included two subsystems, the Security Management Interface (SMI) and the Security Analysis Package (SAP). The SMI subsystem integrated with network management software to provide a graphical user interface (GUI) and tools to assist a user in monitoring and responding to security events occurring on different NSXs reporting to

[2] The NetRanger documentation uses the terms "event" and "alarm" interchangeably, as do I.

that Director. The SAP subsystem provided additional data management, data analysis capabilities, and the ability to generate reports correlating information from multiple sources. The SAP subsystem could be configured to run on the same platform as the SMI, or run on a separate database server.

35. NetRanger used the BorderGuard security device to copy packets directly off the network and send them to the NSX Sensor for analysis. The BorderGuard device could be configured to send all packets to the Sensor, or a defined subset of the packets. NetRanger included a large variety of signatures to analyze the packets, some of which looked at the structure of the packet headers, and some of which looked at the data being transported in the packet.

36. Different NetRanger signatures indicate that NetRanger monitored at least the following different "categories" of network traffic. These categories of network traffic are called out in '203 patent claim 1 and '615 patent claim 1:

Claimed category	Monitored
network packet data transfer commands	• FTP directories created/deleted (4-79) • FTP files GET/PUT (4-79) • HTTP GET (4-80)
network packet data transfer errors[3]	• IP fragments (4-61) • ICMP unreachable (4-67) • ICMP parameter problem on datagram (4-69) • Failed FTP attempt (4-82)
network packet data volume	• ICMP flood (4-61) • Large ICMP traffic (4-63) • ICMP network sweep (4-63) • TCP port sweep (4-63) • UDP port scan (4-63) • SATAN scan (4-63) • Number of bytes within a TCP connection (4-72)
network connection requests[4]	• Connection request from specific IP address (1-10) • TCP connection requests (SYN packets) (4-63) • Connection requests from various other network

[3] Some of these errors, including "ICMP unreachable" would also constitute "an error code indicating a reason a packet was rejected" as claimed in '338 claim 10.

Claimed category	Monitored
	services (C-4 to C-5) • Failed logins (FTP, telnet and rlogin authentication failures)
network connection denials	• FIN packets (4-72) • RST packets (4-72) • Failed logins (FTP, Telnet, rlogin authentication failure (4-62)
error codes included in a network packet	• multiple types of failed packets and connections (4-82) including failed ping and finger requests
network packets indicative of well-known network-service protocols	• unknown IP protocol (4-61)

37. A fundamental design principle of NetRanger was its modularity. Each of the different services required for the various subsystems were broken apart into their atomic operational components, or daemons. This approach allowed for improved speed, durability, scalability, and independence.

38. NetRanger was also perfectly suited for use in distributed, hierarchical monitoring. As shown in the attached Figure 1 in Exhibit D a single NSX could communicate with more than one Director. In addition, Directors could be configured into a hierarchy of Directors, where more than one Director reported up to a higher-tier Director. As shown in the attached Figure 2 in Exhibit D, the WheelGroup in its training slides explained to customers that NetRanger could operate in a four-tier hierarchy, with the NSX sensors serving at the lowest level collecting and analyzing network traffic. Events from these NSXs would be passed to a set of Directors at Tier 3 providing local network security management. A desired set of events, or all events, depending on user preferences, could also be passed up to a smaller set of Directors at Tier 2, which would consolidate information across multiple local Directors and provide regional management. Finally, regional Directors could pass information to a single overall

[4] The NetRanger software included a TCP stream reassembly engine used for many of the NetRanger signatures. This engine would monitor network connections using "a correlation of network connections requests and network connection denials" as claimed in '338 claim 7.

Director at Tier 1, which would further consolidate information and provide enterprise-level management.

39. In the spring of 1997, the DoD/SPOCK analysis was performed to test the capabilities of the NetRanger system. NetRanger was tested in an operational environment over a seven site network connected via an Internet based virtual wide area network (WAN). The WAN was comprised of Internet connections between the following sites: Army Battle Command Battle Laboratory (BCBL) at Fort Gordon, Georgia; NSA/V2 at Fort Meade, Maryland; Air Force Information Warfare Center in San Antonio, Texas, Center for Integrated Intelligence Systems (Space and Naval Warfare Systems Command) in McLean Virginia, Fleet Information Warfare Center, Norfolk, Virginia, and Land Information Warfare Activity, Fort Belvoir, Virginia. An NSX and a Director was placed at each of these sites. In addition, a Director was placed at COACT Inc. (NSA) in Columbia Maryland; to provide global monitoring at all sites.

40. NetRanger also provided automatic integration and correlation of event/alarm data generated from the analysis of network traffic. The Director automatically integrated multiple alarms in certain situations to reduce and consolidate the amount of data presented at the Director level. For example, a TCP port sweep over a variety of source-destination port pairs would be integrated into a single alarm icon. Not every packet received would be used to generate an Alarm icon on the Director – the alarm had to exceed a defined severity threshold. Furthermore, if two or more alarms were received that were similar in all respects except for their timestamp and alarm identification number, the Director would consolidate these multiple alarms into a single "Alarm set" icon.

41. Detection of a SATAN attack also required NetRanger to correlate different events to determine that indeed a SATAN attack was occurring. The NetRanger Sensor would recognize and track multiple different events occurring at different times, such as a ping sweep alarm and a later port sweep. The NSX would keep track of these

multiple different events as they occurred, and when appropriate would generate a SATAN attack event based upon the correlation of the occurrence of these events.

42. The NetRanger Director SAP subsystem also provided automatic correlation of event data. SAP was shipped with a set of comprehensive SQL queries to analyze data based upon different perspectives. These queries could be customized to automatically run periodically and generate different reports of events. For example, the Space Dimension queries would correlate events based upon where the attacks came from, allowing a user to see, for example, the "top ten addresses generating attacks" on the system being monitored. The Time Dimension queries would correlate events based upon when events occurred. The Events Dimension queries would correlate events by linking related attack types and related alarm severity levels.

43. I currently have a working version of the NetRanger 2.1 product in binary form. The 2.1 version of NetRanger, released in January 1998, was functionally identical to NetRanger Version 2.0 in all relevant aspects. The only differences were the additional of more attack signatures, and some minor bug fixes. At trial, I may rely upon this code or a similar version to demonstrate the relevant features of the NetRanger product.

VI. COMMERCIAL SUCCESS OF NETRANGER

44. Commercial intrusion detection systems first began to appear in the 1990s. It is often difficult to cleanly distinguish between a network intrusion detection system and many other network systems that perform some type of security function, such as network monitoring and management software, or the wide variety of firewalls in existence in the 1990s. Nevertheless, I think it is fair to say that the WheelGroup, founded in 1995, was one of the first companies to develop a commercially viable network intrusion detection system. WheelGroup's primary competitor in the market in the 1996-1997 timeframe was the ISS RealSecure product.

45. Sales of NetRanger were good. WheelGroup customers include the US Air Force, US Navy, IBM, AT&T, Storege Tek, Network General, BTG, Perot Systems, Alcatel, CDW, Boeing, Procter and Gamble, Citibank, CompuServ, Chrysler, Allstate, and many others. A WheelGroup customer list dated January 5, 1998 lists 65 customers using NetRanger. Twenty of those companies were in the Fortune 500.

46. Commercial partners of WheelGroup also used NetRanger in services offerings to their customers. Such companies would use the NetRanger product to monitor their customer's network, typically with a Director back at the service company's headquarters to provide real-time monitoring of each customer's network. For example, the ProWatch Secure service offered 24-hour monitoring of traffic on Internet gateways using NetRanger. IBM network services also purchased NetRanger for use as a monitor/sensor in their service offerings.

47. In addition to commercial sales to customers, the NetRanger product was also purchased and used by the U.S. Government. For example, in approximately July 1996, the 609th Information Warfare Squadron located at Shaw Air Force Base (AFB) spent approximately $800k to purchase the NetRanger system to protect US Air Force computer networks.

48. Eventually in March 1998, Cisco Systems Inc. purchased the entire WheelGroup Corp., including the NetRanger product line, for $124 million in stock. Cisco's primary reason for purchasing WheelGroup was its desire to obtain the NetRanger product in order to have a commercially viable network intrusion detection offering, which helped round out Cisco's other networking product offerings. This sale of the company to Cisco demonstrates the desirability and commercial success of the NetRanger product. Cisco changed the name of the product to the "Cisco Secure Intrusion Detection System" for marketing reasons. NetRanger code and technology is still used in the product today and many of WheelGroup's software developers are still employed by Cisco to continually improve the product.

49. I believe that the WheelGroup NetRanger product was successful for two reasons: the product worked as advertised and it was very reliable. NetRanger successfully passed operational tests time and time again by reliably detecting network attacks. It was able to operate continuously over a period of months without crashing. I remember that some of our customers, including IBM ERS, purchased NetRanger after they had already purchased the ISS RealSecure product because our system was so reliable.

VII. LACK OF NOVELTY

50. I understand that a patent is not valid if it can be shown by clear and convincing evidence that the inventions disclosed in the patent are not new and novel. An invention is not novel if the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States.[5] The effective filing date for all of the patents-in-suit is November 9, 1998.

51. In order to demonstrate a lack of novelty, an invalidating prior art reference must disclose each and every limitation of the claimed invention, either expressly or inherently, in detail sufficient to enable one of ordinary skill in the art to practice the claimed invention without undue experimentation. For the purpose of this analysis, I was asked to assume that one of ordinary skill in the art in 1997 would have been someone with an undergraduate degree in Computer Science with at least three to five years experience in computer programming and network design with an emphasis in network monitoring technology and intrusion detection.

52. As shown in the chart attached as Exhibit E, it is my opinion that the NetRanger User's Guide Version 1.3.1 is a printed publication prior art reference that invalidates claims 1-22 of U.S. Pat. No. 6,484,203 and claims 1-6, 8-23, 34-53, 64-73,

[5] 35 U.S.C. sec 102(b).

and 84-93 of U.S. Pat. No. 6,711,615. In addition, as shown in the same chart, the NetRanger product itself circa November 9, 1997 also demonstrates that the alleged inventions described in these claims were in public use and on sale more than one year prior to the date of application for these patents.

VIII. OBVIOUSNESS

53. In addition to the requirement that a patent claim be novel, I understand that a patent claim is presumed valid unless it is shown by clear and convincing evidence that the differences between the subject matter claimed and the prior art were such that the subject matter as a whole would have been obvious to a person having ordinary skill in the art to which the subject matter pertains.[6]

54. I understand that in determining the obviousness of the claim(s) of a patent, one should consider:

a. the scope and content of the prior art relied upon by the party alleging invalidity of the patent;

b. the differences, if any, between each claim of the patent and the prior art; and

c. the level of ordinary skill in the pertinent art at the time the invention of the patent was made; and

d. whether the prior art enabled a person of ordinary skill in the art to make and use the invention claimed.

55. I understand that one must also consider such objective considerations as commercial success, long-felt but unresolved need, failure of others to solve the problem, acquiescence in the patent by others, and whether the same or similar inventions were made independently by others prior to or at about the same time as the invention claimed in the patent.

56. I understand that the test of obviousness is whether the claimed invention, as a whole, would have been obvious to one of ordinary skill in the art as of the date of

[6] 35 U.S.C. sec 103.

the invention in light of the prior art. To establish obviousness under this test, I understand that one must show by clear and convincing evidence that a person of ordinary skill in the art at the time of invention, confronted by the same problem as the inventor and with no knowledge of the claimed invention, would select the recited elements from the prior art and combine them in the claimed manner. In other words, one must avoid the use of hindsight and instead identify in the art prior to the invention some suggestion or motivation, before the invention itself was made, to make the new combination.

57. I understand that the motivation to combine prior art references need not be expressly stated in the prior art, but that it may be found, for example, in the nature of the problem to be solved, or may come from the knowledge of those skilled in the art.

58. As described previously, the NetRanger NSX component correlated different attack signatures to determine whether or not a SATAN attack was occurring. It would have been obvious to perform this correlation at the Director as well. One of skill in the art would have been motivated to make this minor change in order to facilitate detecting a SATAN attack occurring across multiple NSX sensors.

59. The NetRanger system looked for patterns in network traffic indicative of known attacks. However, it was well-known in the intrusion detection field at the time that one might also monitor a network to try and detect behavior that appeared anomalous, or different, from the normal behavior of the network. Often referred to as "anomaly detection," these methods were supposed to be able to detect unknown attacks that deviated from normal activity but did not match any known attack pattern.

60. The use of statistical profiling for performing anomaly detection was well-known by November 9, 1997. By that time, SRI had published extensively on the use of statistical profiling in NIDES (Next-generation Intrusion Detection Expert System).[7] SRI

[7] *See, e.g.*, A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES (Next Generation Intrusion Detection Expert

had also published on the EMERALD system.[8] It had been suggested by many researchers in the field at the time that it was desirable to combine both signature-based detection to look for known attacks with anomaly detection to look for potentially unknown attacks. Thus, it would have been obvious to one of ordinary skill at the time to combine a statistical profiling method for anomaly detection such as those described in *Statistical Methods* and *Emerald 1997* with the NetRanger system if commercial-grade software implementing such an anomaly detection system had existed in 1997. Therefore, as indicated in the chart in Exhibit E, U.S. Patent 6,711,615 claim 7 and claims 1-24 of U.S. Patent 6,708,212 are invalid as obvious.

61. However, the needs of a commercial system such as NetRanger were very different than a research system. In particular, when performing real-time network intrusion detection, it was of paramount importance that the software analyzing the network traffic run quickly in order to be able to keep up with the incoming stream of network packets. WheelGroup actually investigated adding such statistical anomaly detection functionality to NetRanger, and based upon our investigation I do not believe a commercial-grade system for statistical anomaly detection existed in 1997 that was suitable for inclusion in NetRanger. However, since we actually considered adding such functionality to NetRanger back in the 1996-1997 timeframe, I believe it would have been obvious to combine NetRanger with a statistical anomaly detection system if one's primary purpose was the creation of a research-oriented system, as opposed to a commercial product.

System)", January 27, 1995 ("*Statistical Methods*") [SYM_P_0068937-SYM_P_0068942].

[8] *See, e.g.*, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Oct. 9, 1997 ("*Emerald 1997*") [SYM_P_0535485 – SYM_P_0535497].

IX. ASIM

62. I helped setup the first monitoring systems for the US Air Force Automated Security Incident Management (ASIM) program. We implemented the first monitoring sites by using the Network Security Monitor (NSM) developed by Todd Heberlein at UC Davis. Initial sites included the Air Force 7th Communications Group located at the Pentagon in Washington D.C. and Wright-Patterson AFB located in Dayton, OH. Both sites were fully operational by the end of 1992. We installed the NSM software on Sun SPARCstations attached to operational Air Force networks. The NSM software at the time included several different types of analysis engines for analyzing network traffic. However, we focused our operations on utilizing NSM's capability to detect specific strings of text within TCP and UDP network sessions. Samples of strings include "login: root" and "GET passwd." Although these examples may seem trivial compared to a modern IDS, they were very effective in detecting unauthorized use of Air Force networks. The success of these early monitoring systems help spur the development of better technologies and operational procedures at the Air Force Information Warfare Center (AFIWC).

Dated: April 19, 2006

Daniel M Teal

Daniel M. Teal

EXHIBIT G

REDACTED

EXHIBIT H

if they just put them in an envelope and mailed them off to the customer. I don't -- I was not involved in that part of operation of net soft.

Q. (BY MR. MILLER) Do you have any of the documents that describe these queries or generation of reports or any cut -- withdrawn.

Do you have any documents that describe NetRanger customers doing custom event correlation?

A. No, I do not have any documents describing how customers would do it. I know they did it, but I didn't ask for copies of their scripts or any of that stuff.

Q. So we just take your word for it that they did it.

MS. BROWN: Objection, argumentative.

A. Yes. I remember -- I stated that I remember IBM ERS having custom scripts, I remember net soft doing custom things. To the best of my recollection, I don't have any proof, but --

Q. (BY MR. MILLER) Okay. No documents?

A. I do not have the documents in my possession.

Q. Up under September 8 through 14th, who

the system. We had timestamps of what event occurs.

Q. (BY MR. MILLER) We've gone down that list. A human operator would look at the output?

MS. BROWN: Objection, vague as to output, calls for speculation.

A. You could have a human operator look at the output. It was not required. It depends upon how you ran the SQL queries.

Q. (BY MR. MILLER) Are you aware of any deployment of NetRanger where a machine further processed the output of a query to perform automatic correlation?

A. To the best of my recollection, I believe that the IBM emergency response services and NetSolve in their business models had automated SQL queries running on the system to generate stuff.

Q. They had the queries automated. I'm talking about the processing, further processing of the query to do correlation. Are you aware of any deployment where the queries were further processed automatically by a computer to perform correlation?

MS. BROWN: Objection, vague, incomplete hypothetical, calls for speculation.

A. From that, I am aware that IBM and NetSolve had separate scripts that could run. It is

the best of my recollection that they could take the output from that and run it through scripts which could then be automated as to -- I do not have copies of those scripts, I do not have copies of the SQL queries that they ran. I am aware that they liked using the NetRanger system because it's so configureable they could do things like that.

Q. (BY MR. MILLER) Did Mr. Gallen provide you with any -- any information to support your view?

A. Mr. Gallen.

MS. BROWN: I'll just caution the witness, you need to wait until he finishes the question.

THE WITNESS: I'm sorry.

MS. BROWN: Just slow down there. Can you reask the question, please?

Q. (BY MR. MILLER) Sure. Did Mr. Gallen tell you that NetSolve utilized a system that would automatically take data provided in response to a query and perform machine-driven correlation on that data?

A. I do not remember Mr. Gallen telling me that when I talked to him in September. Mr. Gallen was not on -- a technical employee, he was in -- I

testimony.

Q. (BY MR. MILLER) I want to be really clear on this, sir. You have absolutely no documentation that shows automatic processes of SQL queries to do correlation your integration. Is that correct?

A. I believe I answered that question.

Q. Three times earlier?

A. Earlier that I do not have documentation that shows that SQL queries were done automatically.

Q. Do you have documentation that shows that SQL queries were processed manually?

A. I do not -- the documentation that I have was the SQL scripts that were provided with NetRanger that were up to -- it was left to the customer to either use those and modify those scripts. That is a documentation that I provided. I do not have any documentation stating how a customer may or may not have used those scripts or have written other scripts.

Q. You have no evidence of any other scripts being written by a customer?

A. I have no physical evidence that I can provide that customers used to do that.

Q. You have no evidence of the results of

your entire file to Symantec's counsel?

A. I did not initially turn over all my files. I did as a result of the subpoena, with the exception of the NetRanger source code that I still have that I mentioned previously that is still owned by Cisco Systems.

Q. Did you provide to Symantec's counsel manuals for BorderGuard?

A. Yes, I did.

Q. When did you do that?

A. I do not remember the exact dates. We would have discussions and I would mention that I had a manual and they wanted a copy of it.

Q. Was it in the September time frame or more recently ?

A. It may have been in September. I honestly do not remember when I gave them copies of those manuals.

Q. You mentioned that you spoke to two of your former colleagues over lunch?

A. Yes.

Q. And who were they?

A. That was Mr. Jerry Lathem and Mr. Kevin Wiley.

Q. And when did you speak to the other

Q. I think you might be talking about Exhibit C.

A. C, yes.

Q. All right. Point me to where it identifies the version of NetRanger that each these customers bought.

(Witness reviewing document(s).)

A. This one, I do know that if the date -- I would have to quarrel -- look at or correlate the dates of when the sale occurred as to when we had the versions of NetRanger that were released based upon what was in the user's manuals. When we sold a product to a user, we shipped them the latest version. All of our customers, the majority, I can't say all, but the majority of them purchased maintenance agreements with WheelGroup corporation such that when they would purchase a version, they were on maintenance and they got every new version that we shipped.

Q. Exhibit C does not --

A. Hmm?

Q. Exhibit C does not -- I'm going to try to do it so you don't --

A. Sorry about that.

Q. Okay. Exhibit C does not state which

version of NetRanger the customer purchased. Is that correct?

MS. BROWN: I'll object, the document speaks for itself. Also ignores his previous testimony.

A. It does not state explicitly which version of NetRanger was shipped to the customer on the date that it was -- that the customer purchased it.

Q. (BY MR. MILLER) Okay. Let's turn to the last page of Exhibit C, C-11.

THE VIDEOGRAPHER: There's five minutes left on this tape.

Q. (BY MR. MILLER) Why did you include Exhibit C-11?

A. This was our first commercial sale of NetRanger.

Q. Which version was this?

A. Based on a time frame, I would say that this is Version 1.0 of NetRanger.

Q. It doesn't say which version NetRanger?

A. It says it right here, NetRanger single tear Director Version 1.0.

Q. Ah, okay. Thank you. What evidence do you have that Version 1.3.1 of NetRanger was offered

Exhibit 465, which is SYM_P_74722-723. Is this the press release you were referring to?

A. Yes, Exhibit 465 is the press release that I was referring to.

Q. Do you have any document showing an offer for sale of 1.3.1?

A. To my knowledge, I do not have a document saying Version 1.3.1 was offered for sale. When I issued the original invoice we previously discussed that was dated 1996, that was Version 1.0. This was in August of 1997, this was Version 2.0. We offered versions from 1.on, 1.2, 1.3, up to 2.0 over that whole time period, therefore I am implying that Version 1.3.1 was offered for sale.

Q. Do you have any evidence that Version 2.0 was ever sold?

Q. (BY MR. MILLER) ?

A. The evidence I would point to would be the sales and looking at for our customers that had maintenance agreements, they would receive copies of NetRanger 2.0 if they were running an earlier version. If they purchased it after August 1997, we would ship them Version 2.0.

Q. So you're relying on this press release, Exhibit 465, to say that any sale reflected on

prior to the 2.1 version, I could use that one for demonstration also.

Q. Okay. In paragraph 15, what evidence do you have that the 1.3.1 user's guide was actually provided to any customer?

MS. BROWN: Objection vague.

A. That's my own -- we had the user's manuals. My recollection is that if someone wanted the manuals when they were considering purchasing our system that we would give those manuals to them.

Q. (BY MR. MILLER) Do you have a recollection of any potential customer ever asking for a user's guide?

A. I do not remember any potential customers asking because I was the chief scientist. I wasn't the sales or marketing guy that was trying to land that customer account.

Q. And you have no evidence that version 1.3.1's user manual was ever provided to any customer, right?

A. Well, the 1.3.1 user's manuals were provided with our product, so customers that purchased our 1.3.1 version of NetRanger would therefore have copies of our user's manuals.

Q. And you have no evidence of an actual

purchase of 1.3.1.

MS. BROWN: Objection, misstates testimony.

A. I, as stated before, I have not found in my files an invoice for a customer purchasing Version 1.3.1. I provided a copy of an invoice for Version 1.0 of the software with maintenance for one year, I believe it was one year, and if I remember correctly I believe they extended that past that date and customers who had maintenance received upgrades. Upgrades would include both software as well as the documentation.

Q. (BY MR. MILLER) Do you have documentation showing that an upgrade customer would get upgraded software and documentation?

MS. BROWN: Objection, calls for speculation.

A. I do not know. In the files that I provided for the subpoena, there may or there may not be a file that showed that we shipped an upgrade to a customer. I do not know. There were numerous files to go through those. I mean, it was not my job. That was for -- you know, I was the chief scientist of the company, building the technology.

Q. (BY MR. MILLER) I understand, sir. I'm

not challenging that at all. I'm just trying to figure out what we have here, like in your expert report, and I don't recall seeing any evidence except that you -- that you point to except, really, the press release. So I'm looking to see if you cite to any invoices showing a sale that would say that this user manual actually went to a customer.

A. What I meant in my expert report is by providing the invoice for Version 1.0 showing a customer purchasing our 1.0 version in 1996, providing that extensive list of customers purchasing our product on the dates, yes, it does not have the actual versions that were shipped to them. I am stating that as a small software company we would ship them the latest stuff that we'd have, and once they bought it we continued to ship them upgrades. I do not have shipping documents, to my knowledge. As stated, I do not have invoices saying they bought Version 1.3.1, but as stated, I do have for version Version 1.0 with maintenance on that.

Q. Okay. If you could turn to Exhibit C to your report, and just the first page is fine. My question is what the last columns mean and you can just give it to me in a narrative if you'd like, starting with NSX P

remember which, what those references are.

Q. To determine whether any of the claims were invalid, did you compare the claims to the prior art?

MS. BROWN: Objection, vague.

A. I compared the claims primarily to the NetRanger system.

Q. (BY MR. MILLER) When you say you compared the claims to the NetRanger system, what precisely did you compare the claims to? I want to know exactly what you mean by NetRanger system.

A. I compared the claims to awful my knowledge to NetRanger being the original author, architect, original coder of the NetRanger system, being a founder of WheelGroup, going through the user's manuals, refreshing my memory, going through all the documentation that we've discussed here today, and going through that to me it was apparent there were the -- when I reached those conclusions, that's why I said NetRanger was already doing what I stated NetRanger was already doing.

Q. Based on your knowledge of the product as a coder of the product, correct?

A. Correct, based upon my knowledge as the inventor of the system, of the NetRanger system --

Q. Based on all of the documents taken together?

A. Based on all of the documents taken together.

Q. Okay.

A. You know, that also includes my memories of customers using the system.

Q. I see. So undocumented memories of customer applications of NetRanger, that was included as well?

MS. BROWN: Objection, calls for speculation.

Q. (BY MR. MILLER) You included undocumented recollections of NetRanger deployments by NetRanger customers in your invalidity analysis?

MS. BROWN: Objection, calls for speculation. The document speaks for itself, if you'd care to point him to anything that you are alleging is in the expert report.

A. For the undocumented memories that we were discussing goes back to those SQL queries which we have already discussed.

Q. (BY MR. MILLER) Okay. If you could turn to Exhibit D of your report, and if you could turn to page 74986 of Exhibit 464 as well. My question,

statistical engine with NetRanger, you conclude that the combination of that technology and NetRanger is or is not obvious?

A. I'd point out the fact that I tried to use another package and integrate it into NetRanger. They quickly became apparent that it wouldn't work. Based upon that experience, you know, I thought of is there anything else that could have worked for a commercial system, there was nothing there. I would have had a different answer if I were a university researcher and I was building a system for research where I'd be presenting papers at technical conferences on it. Then I may have included it.

Q. What evidence do you have that WheelGroup ever considered incorporating statistical anomaly detection in NetRanger?

A. We tried to incorporate the Haystack Labs NetStalker product in NetRanger. I don't know what documentation I may have.

Q. Do you cite to any in your report? You talk about this at paragraph 61, if that helps you. And I'll represent to you that you don't cite to any documents to support that.

A. Again, I don't know if I provided any documents.

read to me, paragraph 56. In other words, one must avoid the use of hindsight and instead identify in the art prior to the invention some suggestion or motivation before the invention itself was made to make the new combination?

MS. BROWN: That statement.

Q. (BY MR. MILLER) So please provide me with the suggestion or motivation found in NetRanger to combine it with the SRI work?

MS. BROWN: Counsel, as you've just pointed out, paragraph 56 doesn't refer to NetRanger. It refers to the prior art.

MR. MILLER: Your objection is noted. Your objection is noted.

A. You know, in there, I am not stating with regards to NetRanger in paragraph 56. I state in paragraph 61 that I attempted to integrate the statistical analysis engine in NetRanger and did not do so.

Q. (BY MR. MILLER) Other than your purported attempt to integrate a statistical anomaly detection engine into NetRanger, what documentary evidence do you have to show a motivation or suggestion to combine NetRanger and a statistical analysis engine?

A. I do not have the documentation that would provide combining NetRanger with the statistical analysis detection engine. I was not part of the financial team. I'm sure there are some legal -- I mean, at WheelGroup, we had signed -- we were attempting to sign a contract with Haystack Labs. I don't have a copy of that contract to my knowledge. I would have to refer -- maybe Mr. Smaha has a copy of the documentation involved at that time. That was not my job at WheelGroup. That documentation would show that WheelGroup and Haystack Labs were entering a contractual agreement where WheelGroup would license the NetStalker engine. I do not have copies of that documentation to my knowledge.

Q. What is your understanding of the enablement requirement?

MS. BROWN: Objection, calls for a legal conclusion.

A. Could you please define the enablement requirement?

Q. (BY MR. MILLER) Do you have an understanding as to whether a reference must be enabled in order for it to be used in an obviousness combination?

EXHIBIT

I

DAY CASEBEER MADRID & BATCHELDER LLP

Renee DuBord Brown
20300 Stevens Creek Blvd., Suite 400
Cupertino, CA 95014
Telephone: (408) 342-4551
Facsimile: (408) 873-0220
rbrown@daycasebeer.com

KING & SPALDING LLP

Theresa Moehlman
1185 Avenue of the Americas
New York, NY 10036
Telephone: (212) 827-4397
tmoehlman@kslaw.com

May 30, 2006

VIA FACSIMILE & U.S. MAIL

Howard G. Pollack
Fish & Richardson P.C.
500 Arguello Street, Suite 500
Redwood City, CA 94063

Re: ***SRI International, Inc., v. Internet Security Systems, Inc., and Symantec Corporation***

Dear Howard:

This responds to your letter of May 22 concerning SRI's desire to add claims 74 and 78 to this lawsuit. These claims add the limitation of a Virtual Private Network (VPN) to the hierarchical monitoring system. This combination of elements has not been in issue previously and was not specifically investigated by the Defendants during fact discovery. The Defendants addressed the VPN elements in the context of the '338 patent claims relating to the disclosed statistical algorithm. Moreover, to the extent that Defendants' experts addressed the VPN element in the '338 patent context, SRI's expert, Professor Kesidis, provided no response.

Given the late date, SRI should not be allowed to add new subject matter that cannot be fully investigated during discovery. Thus Defendants object to the addition of these claims.

Sincerely,

DAY CASEBEER MADRID & BATCHELDER LLP

Renee Brown

KING & SPALDING LLP

RDB for Theresa Moehlman

Theresa Moehlman

TAM:mp

DAY CASEBEER
MADRID & BATCHELDER LLP

20300 Stevens Creek Blvd., Suite 400
Cupertino, California 95014

Telephone: (408) 873-0110
Facsimile: (408) 873-0220

FACSIMILE TRANSMISSION

DATE: MAY 30, 2006 **NO. OF PAGES:** 2

PLEASE DELIVER TO:

HOWARD G. POLLACK
FISH & RICHARDSON P.C.

PHONE NO. (650) 839-5070 **FAX NO.** (650) 839-5071

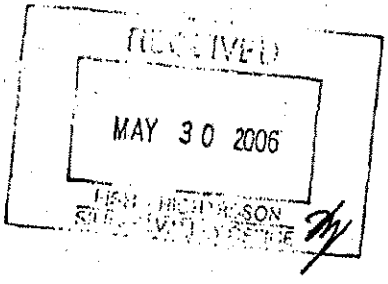
FROM: RENEE DUBORD BROWN

CLIENT NO. : 1904-001

MESSAGE:

PLEASE SEE ATTACHED.

ORIGINAL(S) WILL BE SENT BY MAIL



EXHIBIT

J

REDACTED